BY ORDER OF THE COMMANDER,
36TH AIR BASE WING

36 ABW INSTRUCTION 33-110

1 APRIL 2003

Communications and Information

WORKGROUP MANAGER'S ROLES AND RESPONSIBILITIES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: 36 CS/SCBQ (TSgt Michael White)

Certified by: 36CS/CC (Lt Col Susan T. Pardo)
Pages: 9
Distribution: F

This instruction implements the Workgroup Management guidance outlined in AFI 33-115V1, *Network Management;* AFI 33-115V2, *Licensing Network Users and Certifying Network Professionals;* AFI 33-202, *Computer Security;* 36 ABWI 33-106, *Requesting Unclassified Network User and E-mail Accounts*. Information is a resource critical to readiness; it is a force multiplier and catalyst to the realization of the AF Core Competency--Information Dominance. Decisively managing DoD and Air Force information ensures maximum application of information warfare for military force effectiveness. Military and civilian leaders, and their staffs, at all levels of command, and within every organization, must view information as a strategic resource. This instruction applies to all units assigned to the 36th Air Base Wing and tenant units, and provides specific guidance on Workgroup Management to each unit ensuring an effective and efficient use of information managers and information systems is maintained.

1. General. This instruction outlines the roles and responsibilities of Workgroup Managers (WM) on Andersen AFB. WMs play a vital role in the maintenance and security of the Air Force's newest weapon system--the network. This instruction reinforces the Air Force's efforts to operationalize and professionalize the network---"One Air Force, One Network."

2. Workgroup Managers (WM).

2.1. As an extension of the Network Control Center (NCC) and any appointed Functional Systems Administrator (FSA), WMs are the first line of help in problem resolution for network users. AFI 33-115V1 provides detailed information regarding WM areas of responsibilities as they pertain to both the NCC and network users.

2.2. Unit commanders will appoint WMs in writing (see **Attachment 1**). Any unit with more than one WM assigned will identify a lead WM (see paragraph **2.3.**). The lead WM is the primary focal point for workgroup management issues within their squadron. If only one 3A0X1 occupational series is assigned to a particular unit, they will be the lead WM for the unit. If a unit does not have any 3A0X1s assigned, the most highly skilled WM will be designated as the lead WM.

2.3. Lead WMs ensure a solid WM program is instituted within the unit/staff agency, provide direction to all other assigned WMs and maintain primary access to all tools and permissions granted by the NCC. The lead WM will take responsibility for communications with the Help Desk (HD) on technical issues, and disseminate technical information from the HD to other WMs and users assigned to the unit/staff agency. Ideally, lead WMs are fully trained and certified before assuming their responsibilities. If this is not possible, they will be entered into a mandatory training and observation mode upon assignment. Furthermore, they must complete all required training and certification within 6 months of appointment. Additionally, assigned WMs entered into training/observation mode must show progression of Computer Based Training (CBT) and qualification training on a monthly basis. Lead WMs should ensure users know their assigned WM. Posted signs with WM names and contact numbers in on a public access bulletin board are recommended.

3. Training. WM training will be provided by the NCOIC of WM Training and Development, in accordance with AFI 33-115V2 and PACAF NOSC/NCC Crew Position Training Guide.

3.1. The NCOIC of WM Training and Development is assigned to the Communications Squadron. The position requires a highly trained/skilled 3C0X1/3C2X1. The individual will bear a major responsibility for providing training for all assigned WMs, and act as the liaison between WMs and the Communications Squadron. Additionally, this person will provide staff assistance visits to each unit on a semiannual basis (see **Attachment 2**).

3.2. WMs will attend a 40-hour basic training course, complete core CBTs, serve 6 consecutive months in a WM position and receive training and certification on all required areas in their respective CFETP and/or AF Form 797 before receiving certification in the WM crew position. All inbound WMs that have completed requirements at their previous assignment will go through an initial evaluation and local orientation certification briefing from the NCOIC of WM Training and Development. Upon successful completion, a statement will be annotated on the member's AF Form 623a to certify qualification in the WM crew position. The Communications Squadron or FSAs may provide additional information systems training as needed.

4. Areas of responsibility. WMs' areas of responsibility consist of technical and administrative support of information systems. These areas are separated into several categories: Hardware Support, Software Management, System Security, Records Management, Additional Duties and Problem Resolution.

4.1. Hardware Support. WMs are responsible for the client devices (PCs or workstations) assigned to a unit, staff agency or section (including all peripherals). The line of responsibility stops at the wall connection. WMs have no jurisdiction for any network architecture behind the wall jack to include: switches, hubs or routers installed by Communications Squadron network management personnel. WMs are forbidden to move, power down, disconnect or otherwise configure any network equipment, except under the explicit instruction of network management personnel. Violation of this instruction will jeopardize a WM's certification. WMs will report any suspected network equipment problems to the HD immediately. NOTE: WMs performing duties within the confines of a community of interest functional area LAN should take direction from the FSA.

4.1.1. Information Systems Database (ISD). The ISD is a useful tool for WMs to support the hardware under their control. WMs will have an ISD available at all times. The ISD will contain vital information on each computer assigned to a WM. The following information is the minimum to maintain within the ISD: organization and office symbol, serial number of the computer; computer host name; stand alone or network; make of the computer, processor speed; amount of physical memory; special software; special configuration requirements; operating system; security or service patches installed and classification of the system. WMs are responsible for maintaining the ISD for their assigned area of responsibility. Lead WMs are responsible to provide information to all flight-level WMs for creation, standardization and maintenance of unit-level ISD. WMs will notify their unit ADPE custodian when computer equipment is moved.

4.2. Software Management. WMs are responsible for managing the software on their workstations. This includes software installation, testing and configuration management. Also, WMs will maintain all documentation, license agreements and the original media. WMs must ensure that all software installed on computers is approved for use on Air Force domains. Furthermore, they will ensure the organization does not use any shareware or public domain software. WMs shall, at a minimum, control all licensed and approved software in a manner to preclude copyright infringements (not including enterprise wide licenses). WMs will install updates to software, including service packs and security patches, as soon as they are disseminated for installation by the 36CS. The NCC will provide guidance on updates and installation locations as they are approved.

4.2.1. Configuration Management. WMs are responsible for ensuring all workstations are configured in accordance with the approved NCC configuration standards. WMs will coordinate with the NCC when there are questions about configuration of new software or non-standard software they need to use in their organization. Configuration management ensures remotely managed NCC software updates can be accomplished in a timely and secure manner. WMs will maintain instructions for software that requires special configuration.

4.3. System Security. WMs are directly responsible for system security. This section is broken into three portions: Computer Security, User Licensing and Information Security.

4.3.1. Computer Security. Individual computer workstations are the weakest link in network security. Workstation security will be closely monitored; security demands the highest priority for WMs. The integrity of your systems depends upon it. The local administrator password and account will only be known and shared by WMs. The default local administrator user account should be renamed to provide an added level of security. Passwords will comply with strong password policies. WMs will not add users to the local administrator group on PCs. If a user needs special privileges to run special software or programs, WMs will create a local policy that will allow users to run those programs. Virus scanning software will be on every machine: stand-alone or network. WMs will ensure updated virus definitions are installed on machines in an expedient manner, and report all viruses to Information Assurance (IA) as outlined in AFSSI 5021. WMs will brief all users on minimum-security requirements and follow up to ensure these requirements are met. All security patches and security updates will be applied immediately, unless otherwise instructed by IA. WMs will comply with all additional computer security procedures, not covered here, in accordance with AFI 33-202.

4.3.2. User Licensing. WMs are responsible for ensuring all users have the proper training and clearances to work on computers connected to the network. WMs will ensure all users follow the steps outlined in 36 ABWI 33-106 and complete ABW Form 11, Unclassified Network User and E-Mail Account Application, to receive a network account. User training requirements and procedures for granting network access are outlined in AFI 33-115V2.

4.3.2.1. License Suspension. Procedures for recommending and disputing license suspension are outlined in AFI 33-115V2. The following are some examples of actions that are inconsistent with licensing principles: installing unauthorized software; failure to maintain an acceptable level of proficiency on a critical program; threatening the security of the network via virus propagation; violation of government E-mail or Internet use policies; hacking or attempting to access unauthorized information; and maliciously altering or changing systems files, operating systems or application software without the consent of the WM.

4.3.3. Information Security. Each user is responsible for securing classified information. All users should ensure that classified information is not shared, distributed or processed on a system that doesn't meet the minimum classification standards. WMs will ensure all users are aware of the location of workstations authorized to process classified information and provide them with any additional instructions needed to ensure information security. WMs will immediately notify IA if a security incident occurs on any information system within their unit. In addition, WMs will comply with local reporting procedures for classification contamination that is provided by the IA office and PACAF Pamphlet 31-2.

4.4. Records Management. In accordance with public laws and directives, all official records must be stored and maintained until proper disposition, regardless of the media. Electronic records storage is the joint responsibility of WMs, Functional Area Records Managers (FARM), Records Custodians (RC) and users. WMs are responsible to assist the FARM and RC in establishing an electronic records file plan in accordance with Air Force, DoD and PACAF instructions. The NCC will provide a records storage area for each squadron on a file server, and provide assistance in conjunction with the HD in creating access groups for each squadron. It is the WM's responsibility to create the groups and provide the list of groups to the NCC for implementation. It is also the WM's responsibility to assign the proper individual users to the proper access groups. WMs are responsible for maintaining proper backups of electronic records on a monthly basis as a minimum. Lead WMs will be provided control of the squadron folders for records management. They are responsible for controlling the proper permissions to each group within the squadron. WMs shall assign permissions at group levels and avoid assigning permissions at the user level. The Base Records Manager provides initial training for records management and can provide further guidance on these procedures.

4.5. Additional Duties. In order to provide a successful WM program, WMs may also be assigned the following administrative additional duties.

4.5.1. Computer Systems Security Officer (CSSO). CSSO duties are outlined in AFI 33-202. Lead WMs should be assigned as the unit CSSO. In addition, CSSOs should institute internal reporting procedures for users to report virus attacks, suspicious malicious activity and security violations to the CSSO for subsequent reporting to IA. The CSSO will brief new users about the unit's reporting procedures. Unit CSSO information will be posted in a common area.

4.5.2. Unit COMPUSEC Manager (UCM). UCM duties are outlined in AFI 33-202. In addition, the UCM should include an initial COMPUSEC briefing to new users, along with an annual briefing. UCMs will receive information and training from IA. UCMs will sign off the user's ABW Form 11 verifying the user has completed required IA training. UCMs will post their name and duty phone in a prominent unit area.

4.5.3. Organization Computer Manager (OCM). WMs will function as the OCM. The OCM does not include duties as the Automated Data Processing Equipment Custodian.

4.5.4. Terminal Area Security Monitor (TASM). WMs should also be assigned as the TASM if the unit has classified systems assigned.

4.5.5. Automated Data Processing Equipment (ADPE) Custodian: Many units may find it convenient to have a single point of control over software and hardware resources.

4.6. Problem Resolution. WMs are the first line of defense in resolving user computer problems. WM need to educate their users to contact them for problem resolution. Network users should not be contacting the NCC directly for assistance.

4.7. The following items are minimum administrative tools a WM should maintain for a successful WM program.

4.7.1. Internal Trouble Call Tracking. WMs will maintain a program to internally prioritize and track computer-related problems and provide users with an estimated time of completion for internal trouble calls within their unit. Lead WMs of large squadrons should have a shared trouble ticket database readily available for all assigned WMs to update, closeout and verify the status of trouble calls. At a minimum, the database or program should contain the user's name, nature of the problem, building number, room number, date and time of problem, brief description, WM assigned to the problem and the fix action. Maintaining these minimum categories allows the WM to track trends and share fix actions throughout the squadron or to WMs of other units. After a WM exhausts all available internal resources without success, they should contact the HD for resolution.

4.7.2. Reporting Procedures. WMs are responsible for reporting to the HD any problems that cannot be resolved internally. WMs should provide as much information as possible to assist the HD in resolving the problem. The HD will generate a trouble ticket and should keep the WM informed on problem status. If the WM doesn't hear from the HD in a timely manner, it is their responsibility to follow up with the HD.

4.8. WM and User Interface. Workgroup management is a customer service based duty. As such, WMs must accept responsibility as the primary contact for user information and education concerning standard information systems and associated software. WMs will train users on **commonly used** application software fundamentals to ensure users can effectively interface with respective standard software applications.

5. Web Page Development and Maintenance. Web page development is important to every squadron. Web pages will be maintained by 3A0X1s and/or WMs (this position is normally referred to as the page maintainer) trained on Hyper Text Mark-up Language (HTML). When a 3A0X1 is not assigned, the commander may designate another AFSC to maintain unit web pages. All web pages must be in accordance with DoD policy, AFI 33-129 or any other governing directives. Web page maintainers should ensure the information posted on their web pages is kept up to date. They should coordinate with the web administrator for posting any updates or changes.

6. NCC WM Coordination. Lead WMs will work closely with the NCC on issues that affect a large number of users in their organization. Such issues would include changes to user or global groups, institution of logon scripts within the organization and any changes to user or organizational E-mail accounts. WMs will be assigned permissions or privileges IAW 36 ABWI 33-106. At a minimum, the NCC will provide a WM group that allows for the most liberal privileges available for a WM to accomplish their work without affecting other users or units on the domain. The NCC will provide access to troubleshooting aides (like Microsoft Tech Net) to assist trained and certified WMs in the performance of their duties. WMs should also coordinate with the NCC when new or unusual software is added to systems to ensure configuration management issues are covered and ensure updates will not affect program operation.

JOSEPH F. MUDD JR., Colonel, USAF
Commander, 36th Air Base Wing

Attachment 1

SAMPLE WORKGROUP MANAGER APPOINTMENT LETTER

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS, 36TH AIR BASE WING (PACAF)
UNIT 14003, APO AP 96543-4003

DATE

MEMORANDUM FOR 36CS/SCBQ

FROM: YOUR SQ/OFC

SUBJECT: Appointment of Workgroup Managers (WM)

1. The following individuals are appointed as WMs for YOUR SQ/OFC.

2. An asterisk denotes the lead WM for the organization. The lead WM is the individual that the Network Control Center personnel contact in regards to Communications Tasking Orders, virus updates/hot washes, and all other network user/WM issues.

RANK/NAME	OFFICE	DUTY PHONE	DEROS	HOME PHONE
TSgt Ozzy Osbourne		366-1234	May 04	632-1111
* SSgt Marty Robbins		366-4321	Jun 03	653-5555
SrA Meg Ryan		366-4213	Mar 03	649-1212

3.All WMs are responsible for providing first-level computer support to users within their unit. Failure to perform assigned duties in accordance with 36 ABW policy or published directives may result in removal as a WM.

4. All WMs will complete training requirements necessary to attain WM certification.

5. This letter supercedes previous letters from this organization, same subject.

YOUR CC SIGNATURE

PRIVACY ACT OF 1974 APPLIES - FOR OFFICIAL USE ONLY
(When filled in)

Attachment 2

WM STAFF ASSISTANT VISIT & SELF-INSPECTION CHECKLIST

1. Are unit WMs appointed by the unit commander and does the NCC WM list reflect this appointment?

2. Is the lead WM identified if there is more than one WM assigned to the organization?

3. Do lead WMs have internal reporting procedures for WMs within the organization?

4. Does the lead WM have a software control program instituted for the control of installed software on unit workstations?

5. Are assigned workstations configured to standard configuration management guidelines as directed by the NCC?

6. Are strong administrative passwords enforced for local administrator accounts (eight upper/lower case alpha characters with at least one numeral and special character)?

7. Are any users added to the administrative group on workstations?

8. Is virus-scanning software installed on all workstations within the organization and are permissions assigned to user groups?

9. Are forms identifying the unit's WM, CSSO, and UCM posted in a prominent area?

10. Does the WM have an electronic records program in place for the organization?

11. Has the WM implemented an internal trouble-call tracking program?

12. Does the WM maintain an Information Systems Database of all unit systems?

13. Are WMs responsible for developing and maintaining unit web pages if assigned?

14. Have WMs completed NCC crew position certification requirements?

Attachment 3

SAMPLE INFORMATION SYSTEMS DATABASE

HOST NAME	Org	Off Symb	OS	MAKE/MODEL	SPEED	RAM	CLASSIFIED?	SPEC CONFIG	SPEC SFTWR	NETWORKED?
W67scbq01	36cs	SCBQ	2K	Dell GX240	1.5	128	No	None	None	Yes